REMARKS

Reconsideration of this application is respectfully requested in view of the foregoing amendments and the following remarks. Claims 29-33 are currently pending. Claims 29-33 are rejected. Claims 29, 31, and 33 are amended to further clarify the claims. Claim 30 is amended to provide proper antecedent basis for a limitation. No new matter has been added.

Examiner's Response to Arguments

The undersigned representative acknowledges the Examiner's assertion that the "Applicant's arguments with respect to clams 29-33 have been considered but are moot in view of the new ground(s) of rejection." However, the undersigned representative respectfully traverses the Examiner's assertion "that the applicant did not effectively challenge the Official Notice(s) cited in the previous office actions therefore those statements as presented are herein after prior art." If the Examiner wishes to take Official Notice, then the undersigned representative requests that the Examiner positively assert such Official Notice in another office action.

Title

The Examiner asserted that "The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed. The following title is suggested: Method for Verifying a Ballot Using a Public Key Encryption and Digital Signatures." The undersigned representative thanks the Examiner for the suggestion and has amended the title accordingly.

Rejection of Claims 29, 30, and 33 under 35 USC § 112, second paragraph

Claims 29, 30, and 33 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Examiner asserts that:

> Regarding Claims 29 and 33, Claims 29 and 33 recite ($DS(B_{cast}, s)$, lower case s, and $DS(B_{cast}, S)$, upper case S, where s (S) is best understood to be the private key of the server (system). Examiner requests clarification of the

differences/intended distinction between the system's private key represented as a lower case s and upper S and suggests Applicant's amend the claims to positively recite the intended differences/distinctions. Appropriate correction is required.

For the purposes of examination the examiner interpreted Claim 29 to read "comparing $DS_{received\ token}(B_{cast}, s)$ and ~~at least one of~~ $DS(B_{cast},s)$ ~~and $DS(B_{cast},S)$~~."

For the purposes of examination the examiner interpreted Claim 33 to read "comparing $DS(B_{cast}, s)$ and $DS(B_{cast},s)$ ~~$DS(B_{cast},S)$~~."

Regarding Claim 30, Claim 30 recites the limitation "A digital signature of the aggregation" in claim 29. There is insufficient antecedent basis for this limitation in the claim.

The undersigned representative traverses the Examiner's assertion that claims 29 and 33, need to be amended to define the differences between a lower case letter and an upper case letter in the second position of the digital signature. As recited in the MPEP, "Where an explicit definition is provided by the applicant for a term, that definition will control interpretation of the term as it is used in the claim. *Toro Co. v. White Consolidate Industries Inc.,* 199 F.3d 1295, 1301, 54 USPQ2d 1065, 1069 (Fed. Cir. 1999)" (See MPEP 2111.01 III.) As recited in the specification of the present application, "Throughout this disclosure in labels such as DS(..., C) or DS(...,c), an upper case letter in the second position means a public key, and a lower case letter means a secret or private key, so that in any particular block, this refers to the fact that when a ballot is received for example, the server creates a digital signature of the ballot using the server's secret or private key." (See specification, 0053). Since the use of using a lower case letter or an upper case letter in the second position of the digital signature is explicitly defined in the specification, the definition will control the interpretation and claims 29 and 33 do not need to be amended.

Claim 30 is amended to provide proper antecedent basis for the "aggregation" limitation.

Lastly, the undersigned representative traverses the examiner's interpretation of claims 29 and 33 because the interpretation changes the meaning of the claims. The undersigned representative requests that the Examiner interpret the claims as currently written.

The undersigned representative respectfully requests that the rejection of claims 29, 30, and 33 under 35 U.S.C. § 112, second paragraph, be withdrawn.

Rejection of Claims 29, 30, and 33 under 35 USC § 102(e)

Claims 29, 30, and 33 stand rejected under 35 U.S.C. § 102(e) as being anticipated by US 2002/0077887 to Shrader *et al.* ("Shrader"). This rejection is traversed. Shrader is directed at an architecture for anonymous electronic voting using public key technologies. As shown in Figure 3, Schrader requires three entities for electronic voting: a voting entity, voting tabulator, and voting mediator. In contrast, the methods described in the present application can use two entities for electronic voting: a voting entity and a server (see, e.g., Figure 5 with the voting entity 41 and the server 43). As further explained below, since these two inventions operate using different components, Shrader does not disclose each and every element of the claims recited in the present application.

In order to maintain an anticipatory rejection under 35 U.S.C. §102, a reference must teach each and every element of the claim. *Verdegaal Bros. v. Union Oil Co. of California,* 814 F.2d 628, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) (A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference). Shrader does not disclose "A method for verifying a cast ballot B_{cast} stored in a server, the method comprising: forming a digital signature of B_{cast} using a private key of the server $DS(B_{cast}, s)$; associating the B_{cast} and $DS(B_{cast}, s)$ with a vote serial number VSN; forming a confirmation token, comprising $DS(B_{cast}, s)$ and VSN; making the confirmation token available to a user; receiving a confirmation token made available to a user; extracting $VSN_{received\ token}$ and $DS_{received\ token}(B_{cast}, s)$ from the received token; and for VSN equal to $VSN_{received\ token}$, comparing $DS_{received\ token}(B_{cast}, s)$ and at least one of $DS(B_{cast}, s)$ and $DS(B_{cast}, S)$; if the comparison shows equivalence between the data compared, determining that B_{cast} is verified, wherein a lower case letter in the second position of the digital signature DS( ) means a private key was used to create the digital signature and an upper case letter means a public key was used to create the digital signature" as recited in independent claim 29 of the present application.

Specifically, Shrader does not disclose "associating the B_{cast} and $DS(B_{cast}, s)$ with a vote serial number;" as recited in claim 29 of the present application. The Examiner asserts that Paragraph 0061, Figures 5-6, and Elements 57, 58 disclose this step. These assertions are directed at a ballot request and the return of a ballot to the voting entity (see Paragraph 0061). In contrast, claim 29 of the present application, as recited in the preamble, is directed at "verifying a

cast ballot B_{cast}" which is stored in a server. A ballot request is not the same as a cast ballot. Hence, the Examiner fails to cite where Shrader discloses this step.

Moreover, Shrader does not disclose "forming a confirmation token comprising $DS(B_{cast}, s)$ and VSN as recited in claim 29 of the present application. The Examiner asserts that Paragraphs 0061 and 0063 and Figures 7-8 disclose this step. These assertions are directed at forming a ballot validation message and a verification message, with the ballot validation message containing "identifying ballot information such as the ballot number." (See Shrader, 0063). Shrader does not disclose that the ballot validation message (the asserted token) includes a digital signature of B_{cast}, $DS(B_{cast}, s)$. Hence, the Examiner fails to cite where Shrader discloses this step.

Moreover, Shrader does not disclose "making the conformation token available to a user" as recited in claim 29 of the present application. The Examiner asserts that Paragraphs 0061 and 0063, and Figures 7-8 disclose this step. These assertions are directed at sending an encrypted ballot validation message and a verification message to a voting mediator. (See Shrader, 0063). As defined in the specification, a user refers "to a person on their own terminal which can be a personal computer or other like device on which voting in accordance with the method and system herein is achieved." (See specification, 0019). The voting mediator is not a user but rather a server. Hence, the Examiner fails to cite where Shrader discloses this step.

Moreover, Shrader does not disclose "receiving a confirmation token made available to a user" as recited in claim 29 of the present application. The Examiner asserts that Paragraphs 0061 and 0063, Figures 7-8, and elements 72-74 disclose this step. These assertions are directed at the voting mediator sending "back a signed and encrypted message to the voting tabulator 74 to indicate whether or not the electronic ballot is valid." (See Shrader, 0063). Paragraph 0063 is silent as to what the mediator sends back to the tabulator regarding the encrypted ballot validation message. The voting tabulator is not "receiving a confirmation token made available to a user" but a message indicating whether the electronic ballot is valid. Such a message is not the same as a confirmation token. Hence, the Examiner fails to cite where Shrader discloses this step.

Moreover, since Shrader is not receiving a confirmation token, Shrader does not disclose "extracting $VSN_{received\ token}$ and $DS_{received\ token}(B_{cast}, s)$ from the received token" as recited in claim

29 of the present application. Since the message does not contain the same information as the recited confirmation token, the same information is not being extracting. Hence, the Examiner fails to cite where Shrader discloses this step.

Furthermore, since Shrader is not extracting the same information from the received message, Shrader does not disclose the comparison steps as recited in claim 29 of the present application. Hence, the Examiner fails to cite where Shrader discloses the comparison steps.

Since claim 30 is dependent on claim 29, claim 30 is allowable for the same reasons. Regarding independent claim 31, since this claim contains similar limitations as argued above with respect to independent claim 29, the same arguments apply to independent claim 31.

For at least these reasons, independent claims 29 and 33, as well as dependent claim 30, are patentable over the cited art. Accordingly, it is respectfully requested that the rejection of claims 29, 30, and 33 under 35 U.S.C. §102(e) be reconsidered and withdrawn.

Rejection of claims 31 and 32 under 35 USC 103(a)

Claims 31 and 32 stand rejected under 35 USC § 103(a) as being unpatentable over an article entitled "Design and Implementation of a Practical Security-Conscious Electronic Polling System" by Cranor et al. ("Cranor") Robbins in view of Shrader. Cranor does not teach or suggest "A method for verifying a cast ballot recorded in a server, the method comprising: receiving in a server at least one set of: a cast ballot B_{cast} and a digital signature of B_{cast} formed with the private key of a voter casting the ballot $DS(B_{cast}, v)$; forming: a digital signature of B_{cast} using a private key of the server $DS(B_{cast}, s)$, associating B_{cast}, $DS(B_{cast}, v)$, and $DS(B_{cast}, s)$ with a vote serial number VSN; forming a confirmation token, comprising: $DS(B_{cast}, s)$, $DS(B_{cast}, v)$, VSN, and DS(Aggregation, s), where DS(Aggregation, s) is the digital signature of the aggregation of the associated B_{cast}, $DS(B_{cast}, v)$, $DS(B_{cast}, s)$, and VSN; making the confirmation token available to a user; receiving a confirmation token extracting $VSN_{received\ token}$ and at least one of $DS_{received\ token}(B_{cast}, s)$, $DS_{received\ token}(B_{cast}, v)$, and $DS_{received\ token}(AG, s)$ from the received token; and for $VSN_{received\ token}$ and the corresponding VSN, comparing at least one of: $DS_{received\ token}(B_{cast}, s)$ and $DS(B_{cast}, S)$; $DS_{received\ token}(B_{cast}, v)$, and $DS(B_{cast}, v)$; $DS_{received\ token}$(Aggregation, s), and DS(Aggregation, s); if comparison shows equivalence between the data compared, determining that B_{cast} is verified" as recited in independent claim 31 of the present application.

Specifically, the asserted section of Cranor does teach or disclose "receiving in a server at least one set of: a cast ballot B_{cast} and a digital signature of B_{cast} formed with the private key of a voter casting the ballot $DS(B_{cast}, v)$; forming: a digital signature of B_{cast} using a private key of the server $DS(B_{cast}, s)$" as recited in claim 31 of the present application. The Examiner asserts that paragraph 2 on page 5 of Cranor teaches or suggests these steps. This asserted section recites "the voter to prepare a voted ballot, encrypt it with a secret key, and blind it." This asserted section fails to disclose which secret key is used for encryption. The claim recites that the "digital signature of the B_{cast} formed with the private key of a voter casting the ballot $DS(B_{cast}, v)$" and "forming a digital signature of Bcast using a private key of the server $DS(B_{cast}, s)$" (emphasis added). In claim 31 the digital signatures are created using different private keys, the voter's private key and the server's private key. The asserted section simply recites a secret key and does not recite the possessor of the private key. Hence, the asserted section does not teach or disclose these steps.

Moreover, Cranor does not teach or suggest "associating B_{cast}, $DS(B_{cast}, v)$, and $DS(B_{cast}, s)$ with a vote serial number VSN;" as recited in claim 31 of the present application. The Examiner asserts paragraphs 3 and 4 on page 7 of Cranor as teaching or suggesting this step. These asserted sections disclose voter registration and do not address a cast ballot. Therefore, the asserted sections do not disclose or suggest the claimed association. Hence, the asserted sections do not teach or disclose these steps.

Moreover, Cranor does not teach the confirmation token as recited in claim 31 of the present application. The confirmation token comprises "$DS(B_{cast}, s)$, $DS(B_{cast}, v)$, VSN, and DS(Aggregation, s), where DS(Aggregation, s) is the digital signature of the aggregation of the associated B_{cast}, $DS(B_{cast}, v)$, $DS(B_{cast}, s)$, and VSN;" where VSN is the vote serial number. The Examiner asserts that paragraph 2 on page 5, the last paragraph on page 7, paragraphs 1-4 on page 8, and Figure 1 of Cranor teach or suggest the confirmation token. The asserted paragraphs do not teach or suggest which keys are used to form the digital signatures. Figure 1 does not explicitly teach or suggest which keys are used to form the digital signatures. Regardless, none of these asserted sections form a confirmation token comprising "$DS(B_{cast}, s)$, $DS(B_{cast}, v)$, VSN, and DS(Aggregation, s)." Hence, the asserted sections do not teach or disclose these steps.

Since Cranor does not teach the confirmation token, Cranor cannot teach or suggest the rests of the steps recited in claim 31 of the present application. In addition, Shrader does not cure the deficiencies of independent claim 31 of the present application.

Finally, the Examiner admits that Cranor "does not expressly teach that ballots further comprise vote serial numbers as claimed." The Examiner attempts to modify Cranor with Shrader to teach or suggest this element. However, recognizing after the fact that such a modification would provide an improvement or advantage, without suggestion thereof by the prior art, is an indication of an improper application of hindsight considerations which is not proper criteria for resolving obviousness.

Regarding claim 32, since claim 32 is dependent on claim 31, claim 32 is allowable for the same reasons.

For at least these reasons, independent claim 31, as well as dependent claim 32, are patentable over the cited art. Accordingly, it is respectfully requested that the rejection of claims 31 and 32 under 35 U.S.C. §103(a) be reconsidered and withdrawn.

CONCLUSION

The foregoing is submitted as a full and complete Response to the Office Action mailed March 2, 2006 and early and favorable consideration of the claims is requested. If the Examiner believes any informalities remain in the application which may be corrected by Examiner's Amendment, or if there are any other issues which may be resolved by telephone interview, a telephone call to the undersigned attorney at (202)508-5843 is respectfully solicited. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1458, and please credit any excess fees to such deposit account.

Respectfully submitted,

Dated: June 2, 2006

KILPATRICK STOCKTON LLP
607 14th Street, Suite 900
Washington, DC 20005-2018
Phone 202-508-5800
Fax 202-585-0045

Thomas A. Corrado
Attorney for Applicant
Registration No. 42,439